OPM Data Breaches

What You Need to Know

16 July 2015

What Happened

- **Two Office of Personnel Management (OPM) Breaches:**

(1) Apr 15, personnel data of *4.2 million* current and former Federal employees stolen

(2) Jun 15, OPM discovered additional compromise involving background investigation (BI) records of current, former, and prospective military personnel, federal employees and contractors

  - *21.5 million* individuals including:
    - *19.7 million* BI applicants
    - *1.8 million* non-applicants (e.g., family members, references)

Apr 15 Info
- Full name
- Birth date
- Home address
- Social Security Numbers (SSNs)

Jun 15 Info
Background Investigations for
- Civilian & Military Employment
- CAC Card Credentialing
- Security Clearances

Data Source: OPM

Why it is a concern

- **Current/former Army members may be impacted by these incidents**
- **Stolen information can facilitate identify theft, security and personnel compromises**
- **Information involved in these incidents includes:**

  - Names, Social Security Numbers, Birthdates and Birth Place
  - Residency (current and former addresses) and educational history
  - Employment history
  - Info about immediate family, personal and business acquaintances
  - Health, criminal and financial history provided as part of BI
  - Interview findings conducted by background investigators
  - Fingerprints
  - Personnel info such as assignments, training records and benefits
  - BI software user names and passwords

Compromise of this data presents risk to our Soldiers and Civilians

What this has impacted

OPM temporarily suspended web-based Electronic Questionnaires for Investigations Processing (E-QIP)

- **Recruiting:** A workaround solution for submitting background investigations (BI) for military accessions was approved – resulting in no impact to this mission
- **Civilian Hiring**: Army continues to hire, but at a significantly slower pace for individuals requiring a BI (SECRET and below)
- **Security Clearances:** Army took a strategic pause on submission of new TOP SECRET, TOP SECRET/SCI and periodic reinvestigations
  - ✓ ALARACT 116/2015 authorizes and provides guidance on the conduct of investigation procedures for suitability, CAC credentialing and non-critical sensitive positions requiring up to a SECRET clearance
  - ✓ When the processing system is restored, prioritization of BI's will be based upon mission needs

What Commands & Soldiers Should Do

Stay updated & informed

- ALARACT: 116/2015 (152133Z JUL 15) , 114/2015 (102257Z JUL 15); 094/2015 (121859Z JUN 15)
- STAND-TO! (14 July 2015) http://www.army.mil/standto/
- CHRA e-mail info to Department of the Army Civilians (initially released on 10 July)
- The Army will distro updated OPM information as it becomes available
- OPM remains the primary info source for all – including Soldiers & DAC
- The OPM Incident Resource Center offers information about incident; identity protection, data security & FAQ: https://www.opm.gov/cybersecurity/
- Link also at www.army.mil & www.defense.gov

What Commands & Soldiers Should Do

Watch for the following notifications

- **Breach #1 – Personnel notified by OPM (E-Mail or Letter)**
- **Breach #2 – Notification methods are being assessed for implementation**
- **OPM will provide identity monitoring and restoration services for those affected by Breach #1 https://opm.csid.com (844) 777-2743**
- **OPM will provide a comprehensive suite of additional services for those affected by Breach #2**
- **OPM will establish a Call Center in the coming weeks for those affected**
- **Commands/Soldiers should:**
  - Visit www.identitytheft.gov for information on identity theft response actions
  - Review AT/FP Level 1 Training
  - Check credit reports & contact financial institutions and advise on possible compromise
  - Be alert for targeted spam and phishing attacks
  - Review Social Networking Safety Tips: http://www.cid.army.mil/documents/Lookout/Social%20Network%20Safety.pdf